

Figure 1

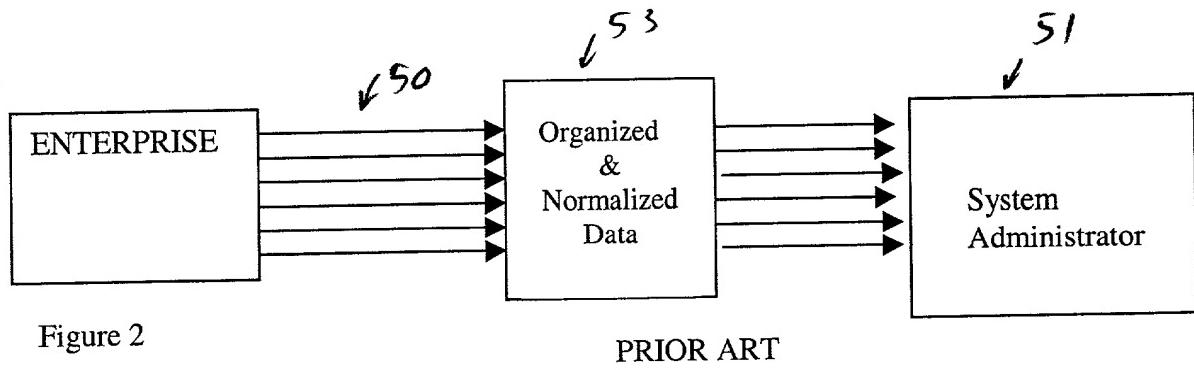
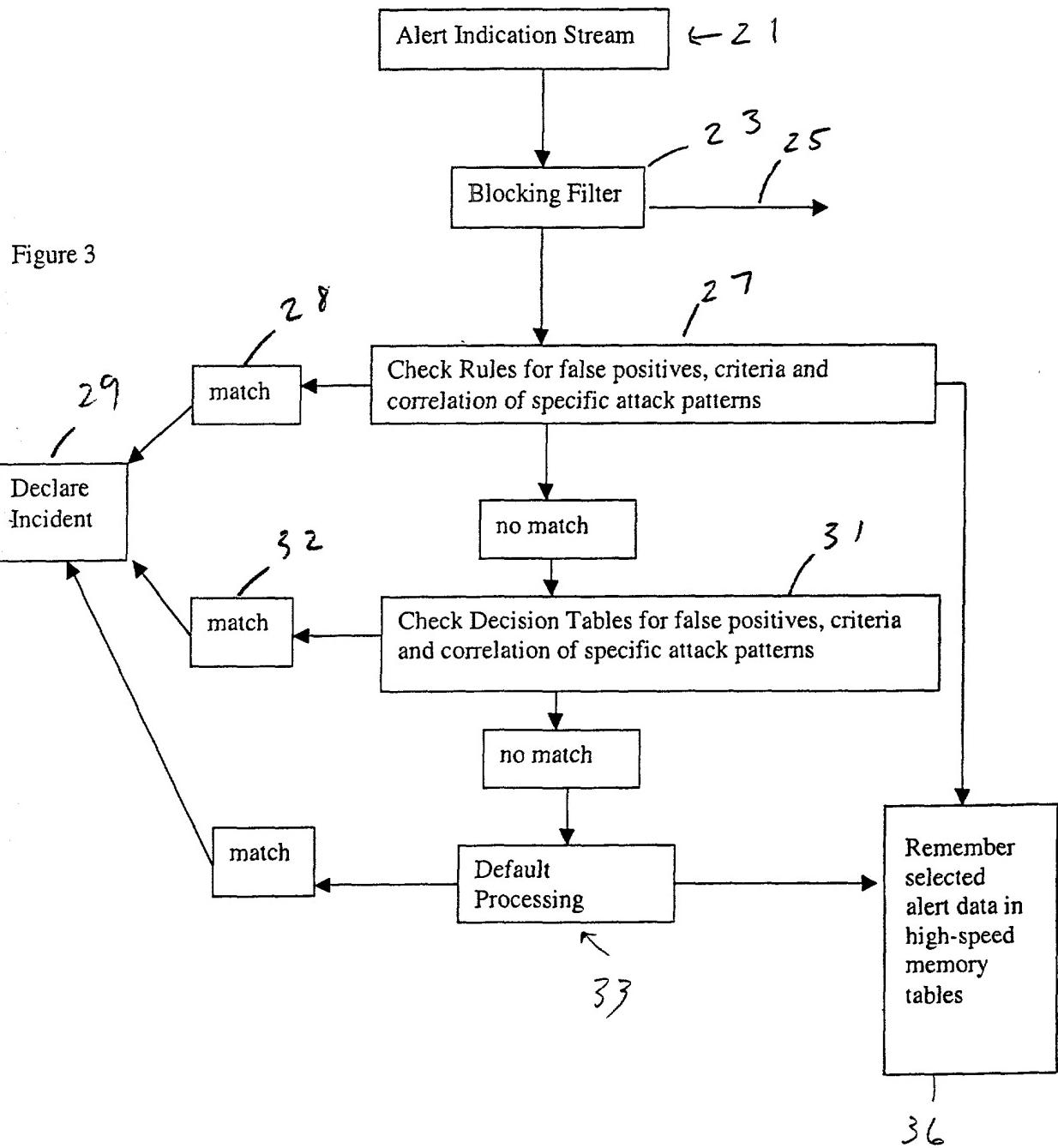


Figure 2



CyberWolf Incident Ticket - Microsoft Internet Explorer

File Edit View Favorites Tools Help

CyberWolf

Incident Ticket ID:1012 Status:Open Priority:Critical

Update Tracking Criteria **Update Incident** **Check History** **Help**

INCIDENT DESCRIPTION

"An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources." ~ AlertType-OS_MultiVendor_noop TrackingSource-10.193.111.87 TrackingTarget-10.193.111.4 Category-OSExploits ExpertType-SnortExpert Severity-1

Date Time	CONCLUSIONS
13:45 02/22/02	"An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources." ~ AlertType-OS_MultiVendor_noop TrackingSource-10.193.111.87 TrackingTarget-10.193.111.4 Category-OSExploits ExpertType-SnortExpert Severity-1
13:45 02/22/02	"An HTML file has been modified on the Web server." ~ AlertType-HTMLFileModify TrackingSource-10.193.111.87 TrackingTarget-10.193.111.87 DeviceIP-10.193.111.87 Category-FileSystemAccess TargetFile-/home/httpd/html/_HomePage.htm ExpertType-ApacheExpert Severity-1
13:45 02/22/02	"An attempt to log in to the host as root failed because the user entered an invalid password or attempted to log in from a remote terminal." ~ AlertType-RootLoginAuthFailure TrackingSource-10.193.111.87 TrackingTarget-10.193.111.87 Category-AuthenticationViolations ExpertType-LinuxExpert Severity-1
13:45 02/22/02	Unauthorized Access Attempt detected on an asset that was recently port scanned - Last scan occurred 1 seconds previous to following alert - "An FTP connection to the host was refused." ~ AlertType-FTPRefused TrackingSource-10.193.111.48 TrackingTarget-10.193.111.87 Category-AuthenticationViolations ExpertType-LinuxExpert Severity-3

Date Time	Agent	ACTIONS
Tracking Rule		
Source:	10.193.111.48	
Targets:	10.193.111.87	10.193.111.4
User Rule	And (TargetPort) Is "2033"	

Date Time	ALERTS
13:45 02/22/02	Description "An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources." From LogSim0 Severity 1 SourceIP TargetIP 10.193.111.4 GenericAlert OS_MultiVendor_noop

[Done]

Fig. 4

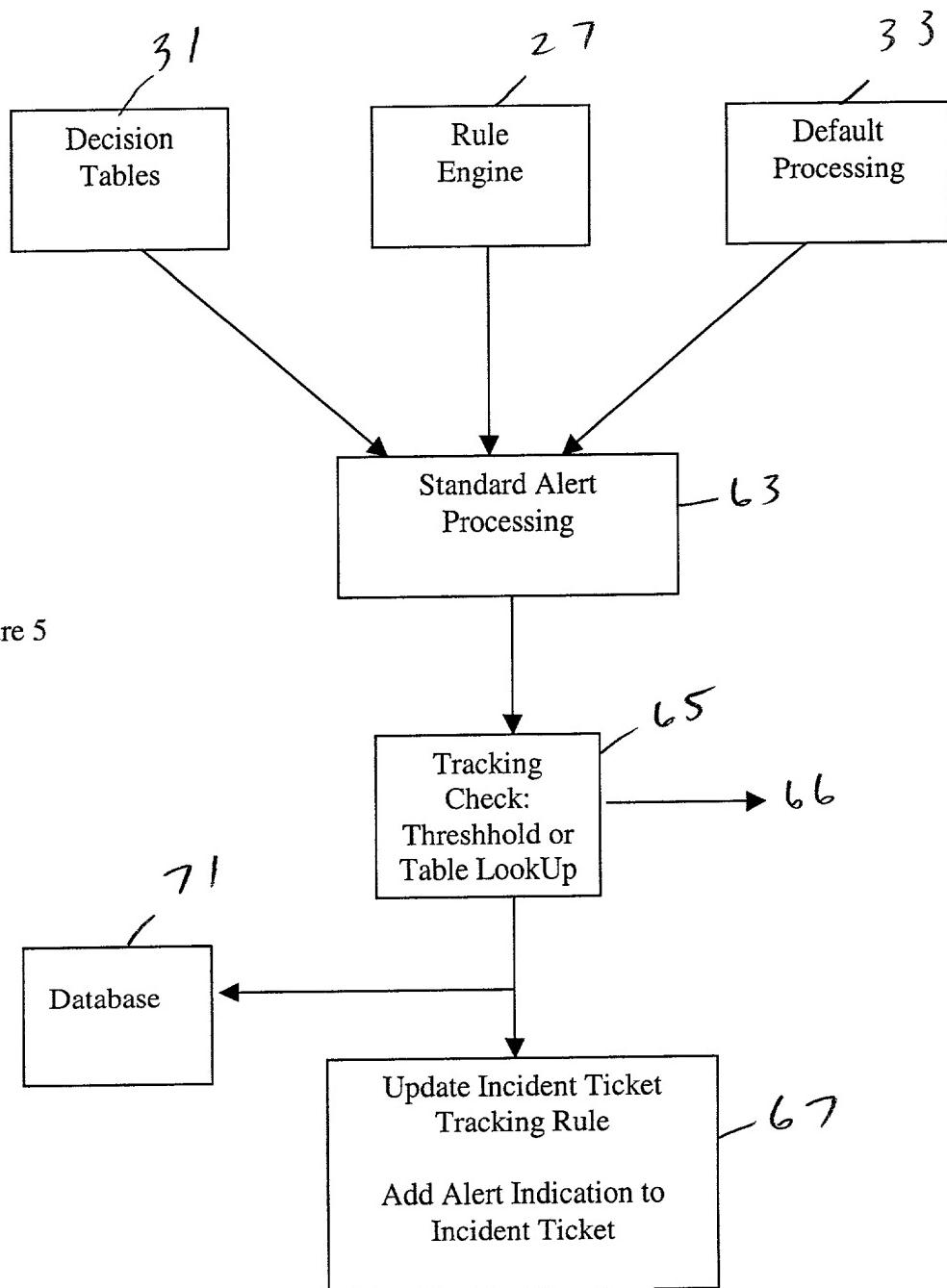


Figure 5

CyberWolf Tracking Criteria - Microsoft Internet Explorer

File Edit View Favorites Tools Help

CyberWolf

Update Tracking Criteria **Incident # 1012**

Disable Auto Update of Tracking Rule Show Details

Source:	10.193.111.48
Targets:	<input checked="" type="checkbox"/> 10.193.111.87 <input checked="" type="checkbox"/> 10.193.111.4
<input type="button" value="Select All"/> <input type="button" value="Unselect All"/>	

	And/Or	(Attribute Name	Condition	Attribute Value)
INS	And	(TargetPort	Is	2033)
DEL						
INS						
DEL						

 Internet

77 71 Fig 6 73 75 ↑ 70